

Aplicação de integridade do banco de dados

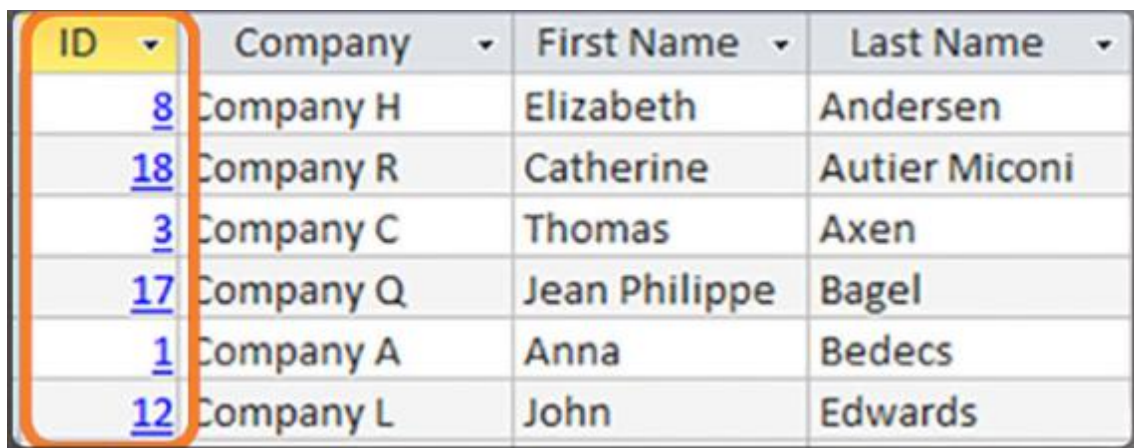
Artigo: Idalécio S.

Segurança da Informação • ISO:IEC 27001 • IT Project Manager • Scrum Master
Publicado • 1 a 16 de setembro de 2022

As bases de dados oferecem uma forma eficiente de armazenar, recuperar e analisar dados. À medida que a recolha de dados aumenta e estes se tornam mais sensíveis, é importante que os profissionais de cibersegurança protejam o crescente número de bases de dados. Pense numa base de dados como um sistema de armazenamento electrónico. A integridade dos dados refere-se à precisão, consistência e confiabilidade dos dados armazenados numa base de dados. A responsabilidade da integridade dos dados recai sobre os criadores da base de dados, os programadores e gestão da organização.

As quatro regras ou restrições da integridade de dados são as seguintes:

- **Integridade da entidade:** todas as entradas devem ter um identificador único chamado Chave Primária (Figura 1)



The image shows a screenshot of a database table. The first column, labeled 'ID', is highlighted with an orange box, indicating it is the primary key. The table contains six rows of data, each with a unique ID, a company name, a first name, and a last name.

ID	Company	First Name	Last Name
8	Company H	Elizabeth	Andersen
18	Company R	Catherine	Autier Miconi
3	Company C	Thomas	Axen
17	Company Q	Jean Philippe	Bagel
1	Company A	Anna	Bedecs
12	Company L	John	Edwards

- **Integridade do domínio:** Todos os dados armazenados numa coluna devem ter o mesmo formato e definição (Figura 2)

Field Name	Data Type
ID	AutoNumber
Company	Text
Last Name	Text
First Name	Text
E-mail Address	Text

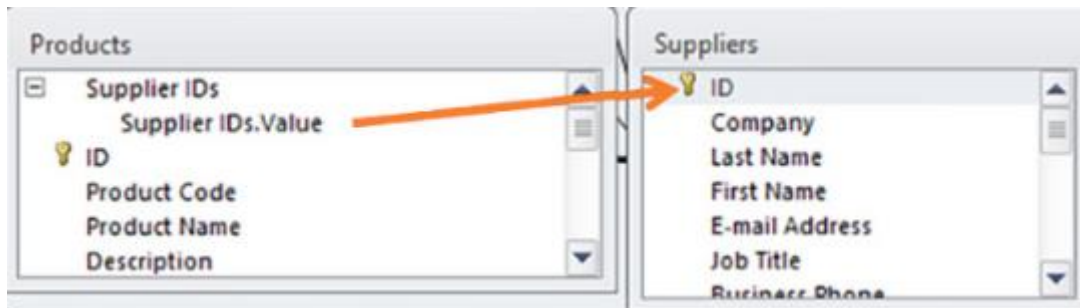
General	
Field Size	50
Format	
Input Mask	
Caption	
Default Value	
Validation Rule	
Validation Text	
Required	No
Allow Zero Length	No
Indexed	Yes (Duplicates OK)

- **Integridade referencial:** Os relacionamentos de tabela devem permanecer consistentes. Por conseguinte, um utilizador não pode eliminar um registo relacionado com outro (Figura 3)

Field Name	Data Type
ID	AutoNumber
Company	Text
Last Name	Text
First Name	Text
E-mail Address	Text

General	
Field Size	50
Format	
Input Mask	
Caption	
Default Value	
Validation Rule	
Validation Text	
Required	No
Allow Zero Length	No
Indexed	Yes (Duplicates OK)

- **Integridade definida pelo utilizador:** um conjunto de regras definidas por um utilizador que não pertence a uma das outras categorias. Por exemplo, um utilizador efectua uma nova encomenda, como se mostra na Figura 4.



O sistema primeiro verifica se este é um novo cliente. Se for, o sistema adiciona o novo cliente à tabela de clientes.

Controles de entrada de dados

A entrada de dados envolve a introdução de dados num sistema. Um conjunto de controlos garante que os utilizadores insiram os dados correctos.

Controlos Drop Down para Dados Mestre

Devem usar uma opção drop down para as tabelas-mestre em vez de pedir aos utilizadores para inserir os dados. Um exemplo do uso de controlos de dados mestres é recorrer à lista oficial de locais (ex., providenciada pelo serviço de correio postal) para normalizar os endereços dos utilizadores.

Controlos de Validação dos campos de Dados

As regras de verificações básicas, incluem:

- A entrada obrigatória garante que um campo obrigatório contenha dados
- As máscaras de entrada impedem que os utilizadores insiram dados inválidos ou ajudam a garantir que eles insiram dados consistentemente (como um número de telefone, por exemplo)
- Montantes positivos em Euros
- Os intervalos de dados garantem que um utilizador insira dados dentro de um determinado intervalo (como uma data de nascimento inserida como 01-18-1820, por exemplo)
- Aprovação obrigatória de uma segunda pessoa (um funcionário bancário recebe um pedido de depósito ou levantamento superior a um dado valor desencadeia uma segunda, ou terceira aprovação)
- Alerta do número máximo de modificações do registo (se o número de registos modificados excede um número predeterminado dentro de um determinado

período, bloqueia um utilizador até que um gestor identifique se as transacções foram legítimas ou não)

- Trigger de actividade incomum (sistema bloqueia quando reconhece a existência de actividade suspeita)

This mockup shows two side-by-side forms on a light blue background. The left form, titled 'Login to your account', includes fields for 'Email' and 'Password', a 'Remember me on this computer' checkbox, a 'Forgot Password?' link, and a 'Log In' button. Below it are two rows of four buttons each, labeled 'Inactive', 'Normal', 'Hover', and 'Pushed', with the bottom row's buttons having a red border. The right form, titled 'Register new account', includes fields for 'Name*' and 'Last Name', 'Address*', 'City*', 'State*', 'Zip Code*', 'Phone Number', and 'Email*'. It features a 'Create Account' button and a 'Cancel' button. A legend at the bottom left of the right form states '* - required fields'.

This mockup shows the same interface as the first one but in Portuguese. The left form is titled 'Faça login na sua conta' and includes fields for 'E-mail' and 'Palavra-passe', a 'Lembrar-me neste computador' checkbox, a 'Esqueceu-se da Palavra-passe?' link, and an 'Iniciar sessão' button. Below it are two rows of four buttons each, labeled 'Inativa', 'Normal', 'Suspensão', and 'Enviada', with the bottom row's buttons having a red border. The right form is titled 'Registrar de nova conta' and includes fields for 'Nome*', 'Apelido', 'Endereço*', 'Cidade*', 'Estado*', 'Código Postal*', 'Número de telefone', and 'Email*'. It features a 'Criar Conta' button and a 'Cancelar' button. A legend at the bottom left of the right form states '*campos obrigatórios'.

Validação do banco de dados

Sobre as Regras de Validação.

Uma regra de validação verifica se os dados estão nos parâmetros definidos pelo programador da base de dados. Uma regra de validação ajuda a garantir a integridade, a precisão e a consistência dos dados. Os critérios usados numa regra de validação incluem o seguinte:

- **Tamanho** — verifica o número de caracteres num campo de dados
- **Formato** — verifica se os dados estão conforme um formato especificado
- **Consistência** — verifica a consistência dos códigos em dados que se encontram relacionados
- **Intervalo** — verifica se os dados estão dentro de um valor mínimo e máximo.
- **Dígito de verificação** — fornece um cálculo extra para gerar um dígito de verificação para detecção de erros

Validação dos dados

A validação do tipo de dados é a validação de dados mais simples, a qual verifica se um utilizador insere dados consistentes com o tipo de caracteres esperado. Por exemplo, um número de telefone não deve conter letras. As bases de dados permitem três tipos de dados: inteiro, texto e decimal.

Validação de entrada

Um dos aspectos mais vulneráveis da gestão da integridade da base de dados é controlar o processo de entrada de dados. Muitos ataques conhecidos são realizados contra uma base de dados, inserindo dados mal formados. O ataque pode confundir, bloquear ou fazer com que a aplicação exponha informação ao atacante. Os atacantes usam ataques de entrada automatizados.

Por exemplo, os utilizadores preenchem um formulário online para subscreverem uma newsletter. Uma aplicação de base de dados gera e envia automaticamente confirmações de e-mail. Quando os utilizadores recebem as suas confirmações por e-mail com um url (link) para confirmar a sua assinatura, esse url foi modificado pelos atacantes. As modificações podem incluir a alteração do nome de utilizador, o endereço de e-mail ou o estado da subscrição. O e-mail retorna para o servidor que aloja a aplicação. Se o servidor Web não verificar se o endereço de e-mail e outras informações da conta recebidas correspondem às informações da subscrição, o servidor recebeu informações falsas. Os hackers podem automatizar este ataque para inundar a aplicação Web com milhares de subscritores inválidos para a base de dados da newsletter.

Verificação de anomalias

A detecção de anomalias refere-se à identificação de padrões nos dados que não estão conforme o comportamento esperado. Estes padrões não conformes são considerados anomalias, outliers, excepções, aberrações ou surpresas, em diferentes aplicações de bases de dados. A detecção e a verificação de anomalias são uma contramedida importante e uma salvaguarda na identificação da detecção de fraudes. A detecção de anomalias na base de dados pode identificar, por ex., fraudes em cartões de crédito e seguros. A detecção de anomalias na base de dados pode proteger os dados contra destruição maciça ou alterações.

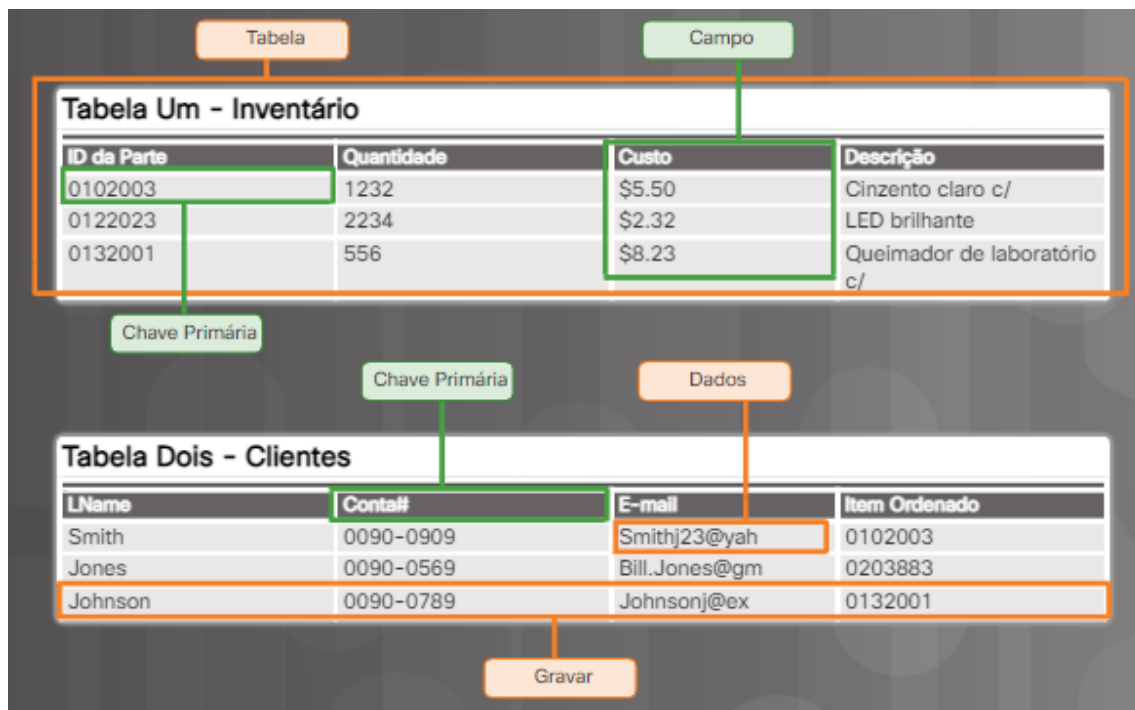
A verificação de anomalias requer a verificação de pedidos de dados ou modificações quando um sistema detecta padrões pouco usuais ou surpreendentes. Um exemplo disto é um cartão de crédito com duas transacções realizadas em locais muito diferentes num curto espaço de tempo. Se um pedido de transacção na cidade de Nova York ocorrer às 10h30 e uma segunda solicitação for de Chicago às 10:35 da manhã, o sistema accionará uma verificação da segunda transição.

Um segundo exemplo ocorre quando um número pouco usual de modificações do endereço de e-mail ocorre num número incomum de registos de base de dados. Como os dados de e-mail são usados para efectuar ataques DoS, a modificação por e-mail de centenas de registos pode indicar que um atacante usa a base de dados de uma organização como ferramenta para seu ataque DoS.

Requisitos de integridade de banco de dados

Integridade da entidade

Uma base de dados é como um arquivo electrónico. Garantir um preenchimento adequado é fundamental para manter a confiança e utilidade dos dados na base de dados. As tabelas, registos, campos e dados dentro de cada campo compõem uma base de dados. Para manter a integridade do sistema armazenamento da base de dados, os utilizadores devem respeitar certas regras. A integridade da entidade é uma regra de integridade, que afirma que cada tabela deve ter uma chave primária e que a coluna ou colunas escolhidas para ser a chave primária devem ser únicas e não NULL. NULL numa base de dados significa valores ausentes ou desconhecidos. A integridade da entidade permite a organização adequada dos dados para esse registo, conforme se mostra na figura.



Integridade referencial

Outro conceito importante é a relação entre diferentes sistemas de armazenamento ou tabelas. A base da integridade referencial são as chaves estrangeiras. Uma chave estrangeira numa tabela referir-se a uma chave primária numa outra tabela. A chave primária de uma tabela identifica de forma única as entidades (linhas) na tabela. A integridade referencial mantém a integridade das chaves estrangeiras.



Integridade do domínio

A integridade do domínio garante que todos os campos de dados numa coluna estejam dentro de um conjunto definido de valores válidos. Cada coluna de uma tabela tem um conjunto definido de valores, como o conjunto de todos os números para os números de cartão de crédito, números de segurança social ou endereços de e-mail. Limitar o valor atribuído a uma instância dessa coluna (um atributo) impõe a integridade do domínio. A imposição da integridade do domínio pode ser tão simples quanto escolher o tipo de dados, o comprimento e o formato correctos para uma coluna.

SSN 243-27-3361	<ul style="list-style-type: none">• Tem que ter nove dígitos inteiros• Formato xxx-xx-xxxx• Introduzido ou modificado apenas pelo cliente• Tem que ser validado
Número de cartão de crédito 4539 4769 0728 4479	<ul style="list-style-type: none">• Tem que ter dezasseis dígitos inteiros• Formato xxxx-xxxx-xxxx-xxxx• Introduzido ou modificado apenas pelo cliente• Tem que ser validado
Endereço de E-mail tortor@odio.com	<ul style="list-style-type: none">• Não pode ter mais do que 128 caracteres• Formato xxxx@xxxx.xxx• Introduzido ou modificado apenas pelo cliente• Validado por resposta de e-mail